Financial Crime, Compliance and Anti-Money Laundering Procedure

Enabling Policy Statement; Executive Owner; Approval Route:	Our Operations - Chief Operating Officer - Operations Committee
Is the Procedure for internal use only (Non-disclosable) ?	Disclosable
Associated Policy Statements:	Our Students - Chief Student Officer
Authorised Owner:	Chief Financial Officer
Authorised Co-ordinator:	EA to the Chief Financial Officer
Effective date:	01/11/2024
Due date for full review:	01/11/2027
Sub documentation:	N/A

Approval History

Version	Reason for review	Approval Route	Date
1.0	Scheduled renewal and updated to new procedure template	Operations Committee	Nov 2024

1. Purpose

1.1. The Financial Crime, Compliance and Anti-Money Laundering Procedure establishes the framework for preventing, detecting, and responding to financial crimes at the University of Surrey.
1.2. The University is committed to upholding the highest standards of integrity and accountability, ensuring compliance with relevant laws and regulations. This policy outlines the principles, risk areas and governance required to manage financial crime risks effectively.

2. Scope and Exceptions to the Procedure

2.1. In the UK, severe penalties can be imposed on both the University and its employees (as individuals) connected with any stage of financial crime and money laundering activities. The University therefore must consider the risks that its business activities will expose it to and devise suitable controls that protect it and its employees against being the victim of any financial crime.
2.2. This procedure documents these risks and aims to guide the monitoring of them on a regular basis. The procedure also considers how it trains its staff to spot potential signs of financial crime and how to report it according to UK law.
2.3. The University also needs to ensure it complies with all local money laundering regulations when it operates overseas.
2.4. This procedure applies to all staff who are engaged in financial transactions for or on behalf of the University.
2.5. Any failure to adhere to this procedure may be dealt with under the University's disciplinary procedures, as appropriate and legal action, if warranted under relevant UK or overseas financial crime related legislation.

3. Definitions and Terminology

3.1. Money Laundering Reporting Officer ("MLRO") is the University Chief Financial Officer
3.2. Know Your Customer ("KYC") checks are a set of procedures that verify the identity of a customer or supplier and ensure they are acting legally
3.3. National Crime Agency ("NCA") is a law enforcement agency in the UK that is responsible for leading the fight against serious and organized crime.
3.4. Suspicious Activity Report ("SARS"), a piece of information which alerts law enforcement that certain client/customer activity is in some way suspicious and might indicate money laundering or terrorist financing.
3.5. Defense Against Money Laundering ("DAML") is a defense against the principal money laundering offences

4. Procedural Principles

4.1. The University's Financial Crime and Compliance Procedure is guided by the following principles:

4.1.1. **Integrity and Transparency**: All financial dealings must be conducted with honesty and openness.
4.1.2. **Compliance:** Adherence to all applicable laws, regulations, and standards related to financial crime.
4.1.3. **Accountability**: Clear assignment of responsibilities and accountability for financial crime prevention and compliance.
4.1.4. **Risk Management**: Proactive identification, assessment, and mitigation of financial crime risks.
4.1.5. **Continuous Improvement**: Regular review and enhancement of procedures and controls to address emerging risks and regulatory changes.

4.2. University risk areas of Financial Crime

The following areas are identified as potential risks for financial crimes:

- **Fraud**: Misrepresentation or deceit for financial gain, including falsification of documents, fraudulent billing, and financial misstatements.
- **Bribery and Corruption**: Offering, giving, receiving, or soliciting anything of value to influence business decisions or gain an unfair advantage.
- **Money Laundering**: Concealing the origins of illegally obtained money, typically by passing it through a complex sequence of banking transfers or commercial transactions.
- **Theft and Embezzlement**: Theft of physical or digital assets, or misappropriation of funds by employees or third parties.
- **Conflict of Interest**: Situations where personal interests may conflict with the University's interests, leading to potential misuse of position or resources.

4.3. Overseas payments often pose higher risk as they can often be made via a third party, can involve the movement of money through multiple bank accounts or involve high risk countries. The University has identified the following key areas which could be exploited by those trying to carry any or all of the three stages of money laundering, above.

- Receiving tuition and accommodation fees from overseas
- Receiving tuition and accommodation fees from sponsors based overseas
- Receiving funds from potentially criminal business entities
- Making refunds to students, and third parties (parents and sponsors)
- Receiving cash transactions (if applicable)
- Receiving donations
- Overseas operations

4.4. University Money Laundering Warning Signs

It is not possible to give a definitive list of ways to spot money laundering. The following are types of risk factors which may, either alone or collectively, suggest the possibility of money laundering activity.

- A new customer, business partner or sponsor not known to the University
- A customer from a country known to carry a high level of risk (such as a sanctioned country, or country with known high levels of financial fraud or corruption)
- A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation.
- A request to pay a substantial sum in cash to the University
- Concerns about the honesty, integrity, identity or location of the people involved.
- Involvement of an unconnected third party without a logical reason or explanation.
- Overpayments for no apparent reason, and requests to pay the difference back to a third party
- Absence of any clear legitimate source for the funds received.
- Significant changes in the size, nature, frequency of transactions with a customer that are without reasonable explanation
- Cancellation, reversal or requests for refunds of earlier transactions.
- Requests for account details outside the normal course of business.
- A history of poor business records, controls or inconsistent dealing
- Receipt of a payment for which the University has not issued an invoice

- A receipt of fees from an unconnected third party (i.e. not a student, family member or sponsor)
- Any other facts which tend to suggest that something unusual is happening and give reasonable suspicion about the motives of individuals.

4.5. Controls

To mitigate the risks of financial crime, the University has the following controls:

Policies and Procedures: Comprehensive policies and procedures for financial operations, procurement, and financial reporting.

Training and Awareness: Regular training programs for staff on financial crime prevention, detection, and reporting.

Segregation of Duties: Financial responsibilities are divided among different individuals to reduce the risk of fraud and error.

Authorization and Approval: strict authorization processes for financial transactions and expenditures.

Monitoring and Auditing: Regular review of financial transactions, internal audits, risk assessments to identify and address potential issues.

Whistleblowing Mechanism: a confidential and secure reporting mechanism for employees and other stakeholders to report suspected financial crimes.

4.6. Due Diligence of funds received

Due diligence is the process by which the University assures itself of the provenance of funds it receives and that it can be confident that it knows the people and organisations with whom it works. In this way the University is better able to identify and manage risk. Due diligence should be carried out before the funds are received. Funds must not be returned before due diligence has been carried out. In practical terms this means:

i) identifying and verifying the identity of a payer or a payee, typically a student or a donor;

ii) where the payment is to come from or to be made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party;

iii) identifying and verifying the source of funds from which any payment to the University will be made;

iv) identifying and in some circumstances verifying the source of wealth from which the funds are derived. Source of funds refers to where the funds in question are received from. The most common example of a source of funds is a bank account. Source of wealth refers to how the person making the payment came to have the funds in question. An example of a source of wealth is savings from employment.

v) The banks and payments portals that the University has partnered with do not accept payments from sanctioned counties thereby preventing the University from receiving these monies.

vi) The University has a robust "Know Your Customer" (“KYC”) process for students and other customers, especially overseas students. Student ID is checked during enrolment, including checks that valid visas are in place where required. Credit checks are performed on sponsors or commercial sponsors via an external credit rating agency (currently Creditsafe) prior to being approved as a customer or sponsor.

In addition to the above the following processes are followed:-

- No cash is accepted for tuition or accommodation fees
- Suspicious payment reports from the University's card payment gateway provider (WPM and Flywire) are monitored daily and investigated where necessary
- No refunds can be made other than to the original payer
- Unallocated payments purporting to be from students are returned to source where no registered student ID is provided and no back up is provided.
- Other than in exceptional circumstances, refunds are only made using the original mode of payment
- Any potential breaches of this procedure must be flagged up to the University's Money Laundering Reporting Officer as outlined below in 2.3.1

4.7. Internal Reporting

It is best practice for universities to appoint a nominated officer or Money Laundering Reporting Officer ("MLRO") to be aware of any suspicious activity in the business that might be linked to all types of financial crime, and if necessary to report it through channels described below.
The nominated officer at the University of Surrey is the Chief Financial Officer.

Where a member of staff knows or suspects that financial crime activity is taking, or has taken place, or becomes concerned that their involvement in a transaction may amount to a breach of the regulations, they must disclose this immediately to their line manager. If in consultation with their line manager reasonable suspicion is confirmed a disclosure report must be made to the MLRO. This disclosure should be made by email and should be completed as soon as possible after the information came to their attention.

The report should include as much detail as possible including:

- Full available details of the people, companies or other entities involved, including the individual making the disclosure and other members of staff if relevant.
- Full details of transaction and nature of each person's involvement in the transaction.
- Suspected type of money laundering activity with exact reasons as to why the individual making the disclosure is suspicious.
- The dates of any transactions, where they were undertaken, how they were undertaken and the likely amount of money or assets involved.
- Any other information that may help the MLRO judge the case for knowledge or suspicion of a financial crime having taken placeand to facilitate his or her report to the relevant authorities.

Once this suspicion has been reported to the MLRO any instructions provided by the MLRO must be followed.

If appropriate the MLRO will refer the case to the UK authorities who will undertake any necessary investigation.

Reports made by a member of staff to the MLRO under the above procedures will be considered for treatment as a disclosure under the University's Public Interest Disclosure (Whistleblowing) Procedure.

4.8. External reporting

On receipt of a disclosure report the MLRO will consider the report and any other relevant information, undertaking further enquires necessary to decide if a report should be made to the National Crime Agency (NCA).

Once the MLRO has evaluated the case a timely determination will be made as to whether:

- There is suspected money laundering taking place
- There are reasonable grounds to suspect that is the case
- A report submission should be made on the SARS website in a timely manner. Details of the reporting to the NCA can be found at https://sarsreporting.nationalcrimeagency.gov.uk/
- In certain cases a Defense Against Money Laundering ("DAML") should also be submitted to the National Crime Agency ("NCA")

Where the MLRO concludes that the case should be disclosed to NCA this will be reported, however if the MLRO concludes that there are no reasonable grounds to suspect money laundering, then consent will be given for transactions to proceed and the disclosure report will be marked accordingly.

Where the MLRO considers a potential breach has taken place, the University may be obliged to report serious incidents to the Office for Students.

5. Governance Requirements

5.1. Implementation: Communication Plan

5.1.1. Finance staff will be notified of the procedure during their onboarding process and the procedure will be available on the policies and procedures page of the University website.

5.2. Implementation: Training Plan

5.2.1. On joining the University any staff whose duties will include undertaking a finance function will receive appropriate financial crime compliance training including anti-money laundering training as part of their induction process. This may include training provided by the British Universities Finance Directors Group (BUFDG) and one to one training from suitably experienced staff.

5.2.2. All staff undertaking a finance function will receive annual refresher anti-money laundering and counter-terrorist finance training. The University's anti-money laundering training will include the applicable law, the operation of this policy and the circumstances in which suspicions might arise.

5.2.3. The University will make and retain for at least five years records of its anti-money laundering training.

5.3. Review

5.3.1. It is good practice to review this procedure every three years.

5.3.2. Minor changes such as change of a role title or other titles or name which do not change the meaning of the procedure may be made by the operational owner. Major changes which alter the meaning of the procedure or are substantial re- writes will be submitted via the full approval route.

5.4. Legislative Context and Higher Education Sector Guidance or Requirements

5.4.1. The laws concerning the various types of financial crime are complex and are increasingly being actively enforced.

i. Proceeds of Crime Act 2002 (POCA): This act criminalizes money laundering and provides law enforcement with powers to seize assets derived from crime. Universities must be aware of their obligations under this law.

ii. Terrorism Act 2000: This legislation includes provisions related to money laundering and requires institutions to report certain financial activities that could be linked to terrorism financing.

iii. Money Laundering Regulations 2017: These regulations implement the EU's Fourth Anti-Money Laundering Directive and set out specific requirements for due diligence, reporting, and record-keeping for designated bodies, including certain higher education institutions.

iv. The UK implements sanctions through the Sanctions and Anti-Money Laundering Act 2018, which allows the government to impose sanctions for various reasons, including national security, foreign policy, and the prevention of terrorism.

v. The Fraud Act 2006 consolidates various types of fraud, including fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.

5.4.2. The University is required to comply with the Proceeds of Crime Act 2002. The University is not authorised or regulated by the Financial Conduct Authority. It therefore does not have to comply with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, but it is considered best practice for it to do so.

5.4.3. UK Financial Conduct Authority (FCA): While universities may not be directly regulated by the FCA, those involved in certain financial activities must comply with its AML requirements.

5.4.4. National Crime Agency (NCA): The NCA oversees the reporting of suspicious activities and provides guidance on AML compliance.

5.5 Sustainability

This procedure has no sustainability impact.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on **22/10/2024** and is held by the Authorised Co-ordinator.

6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	**Nature of Engagement**	**Request EB Approval(Y/N)**	**Date**	**Name of Contact**
Governance	Review of written procedure	N	04/10/2024	Kelley Padley, Governance Officer
H&S	Review of Health and Safety aspects	N	02/10/2024	Matt Purcell, Director of Business Resilience (Cervus Plus Consulting)
Sustainability	Review of Sustainability impact	N	22/10/2024	Martin Wiles, Head of Sustainability
Academic Freedom of Speech	Review of impact on academic freedom of speech	N	04/10/2024	Abigail Bradbeer, Surrey Business School – School Manager
Our Students Policy Statement Area	Associated Policy Statement Review	N	28/10/2024	Kerry Matthews (Chief Student Officer)